FortiClient Configurator Tool

The free FortiClient Configurator Tool is used to create custom FortiClient installation files. Starting with FortiClient 5.6.0, an account for Fortinet Developer Network (https://fndn.fortinet.net/) is required to access the free tool. No license key is required to use the tool.

The FortiClient Configurator Tool is available for Microsoft Windows and macOS operating systems.

Overview

Following is an overview of using the FortiClient Configurator Tool:

1. Log into your FNDN account, and download the tool from FNDN. See Downloading the tool on page 1.
2. (Optional) Prepare configuration files and Telemetry gateway IP lists. See Preparing configuration files on page 2.
   You have the option to add a FortiClient configuration file and/or Telemetry gateway IP list to the FortiClient installer. Before you create the installer, you should get these files ready for selection.
3. Create a custom FortiClient installer. See Creating custom FortiClient installation files on page 4.
4. Deploy the custom FortiClient installation packages. See Deploying custom FortiClient installation packages on page 11.

Downloading the tool

Download the free FortiClient Configurator Tool from the Fortinet Developer Network site.

An account is required to access the Fortinet Developer Network. Information about creating an account is available at https://fndn.fortinet.net/.

To download the tool:

1. Log into your FNDN account at https://fndn.fortinet.net/.
   If you do not have an account for FNDN, you must create an account at https://fndn.fortinet.net/index.php?/register/.
   When you create an FNDN account, you are required to include the email address for two Fortinet sponsors. Fortinet sponsors are Fortinet employees who can verify that you are a Fortinet customer. Contact your sales representative or sales engineer for email addresses for Fortinet sponsors.
2. Go to *Tools* > *Personal Toolkit*, and download the FortiClient Configurator Tool.

Preparing configuration files

You can select the following types of files in the FortiClient Configurator Tool when you create a custom FortiClient installer:

- Configuration file
- Gateway IP list

This section describes how to retrieve and edit the files to prepare them for use with the FortiClient Configurator Tool.

You can use an XML editor to make changes to the FortiClient configuration file and Telemetry gateway IP list. For more information on FortiClient XML configuration, see the *FortiClient XML Reference* in the Fortinet Document Library at http://docs.fortinet.com.

Retrieving FortiClient configuration files

You can retrieve a configuration file from FortiClient. The configuration file contains the settings for FortiClient. After you retrieve the configuration file, you can use an XML editor to make changes to the configuration file. Then you can select the FortiClient configuration file in the FortiClient Configurator Tool.

To retrieve FortiClient configuration files:

1. In FortiClient, go to *Settings*.
2. In the *System* area, click *Backup*.
3. Select a destination, and click *Save*.

Configuring Telemetry gateway IP lists

You can retrieve a configuration file from FortiClient to access the XML elements for the Telemetry gateway IP list.

If you are using FortiClient EMS (Enterprise Management Server), you can export a gateway IP list from FortiClient EMS. See the *FortiClient EMS Administration Guide*.

The Telemetry gateway IP list contains IP addresses for FortiGate and/or FortiClient EMS. FortiClient uses the Telemetry gateway IP list to connect FortiClient Telemetry to FortiGate or FortiClient EMS.

After you retrieve the configuration file, you can use an XML editor to locate the elements for the Telemetry gateway IP list and modify them.

To configure Telemetry gateway IP lists:

1. In FortiClient, retrieve the configuration. See Retrieving FortiClient configuration files on page 2.
2. Open the configuration file in an XML editor.
3. Remove all elements, except the elements needed to configure the Telemetry gateway IP list. See Example XML of Telemetry gateway IP list on page 4.

4. Add IP addresses to the configuration file by using an XML editor.
   When using only FortiGate for endpoint control, use the `<fortigate>` element to identify one or more IP addresses for FortiGate devices.
   When using FortiGate integrated with EMS, use the `<fortigate>` element to identify one or more IP addresses for FortiGate devices, and use the `<notification_server>` element to identify the IP address for EMS.
5. Save the configuration file.

Example XML of Telemetry gateway IP list

Following is an example XML file for a Telemetry gateway IP list. In this example, endpoints will connect Telemetry to FortiGate by using the IP addresses in the <fortigate> element and send notifications to FortiClient EMS by using the <notification_server> element.

```
<?xml version="1.0" encoding="UTF-8" ?>
   <forticlient_configuration>
      <endpoint_control>
         <enabled>1</enabled>
         <disable_unregister>0</disable_unregister>
         <silent_registration>1</silent_registration>
         <fortigates>
            <fortigate>
               <serial_number>fgt_sn0</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                     da7e6495841d8fc9c61067f81ef4cac01d697bb7e160c24d</registration_password>
               <addresses>172.30.254.150:8013</addresses>
            </fortigate>
            <fortigate>
               <serial_number>fgt_sn1</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                     6c9f088323beef31ea969c1c31c6db0e766273cb21851e68</registration_password>
               <addresses>172.30.254.174:8013</addresses>
            </fortigate>
            <fortigate>
               <serial_number>fgt_sn2</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                     7e819fa80a68ca2b602fdad54ba76190f03777c70399471d</registration_password>
               <addresses>172.30.254.158:8013</addresses>
            </fortigate>
            <notification_server>
               <address>us-ems1.myfortinet.com:8013</address>
            </notification_server>
         </fortigates>
      </endpoint_control>
   </forticlient_configuration>
```

Creating custom FortiClient installation files

The following section provides instructions on creating a custom installer file using the FortiClient Configurator Tool.

You have the option to select a FortiClient configuration file and/or Telemetry gateway IP list when you create a custom FortiClient installer. See Preparing configuration files on page 2.

Ensure that you select all modules in the FortiClient installer that you want installed on endpoints. To enable other features after FortiClient is installed, you must uninstall FortiClient from endpoints, and reinstall an MSI file with the desired features included in the FortiClient installer.

If you're using FortiClient EMS to deploy and manage FortiClient endpoints, you can create a FortiClient installer that includes most or all modules, and you can use a profile from FortiClient EMS to disable and enable modules without uninstalling and reinstalling FortiClient.

Using FortiClient Configurator Tool for Windows

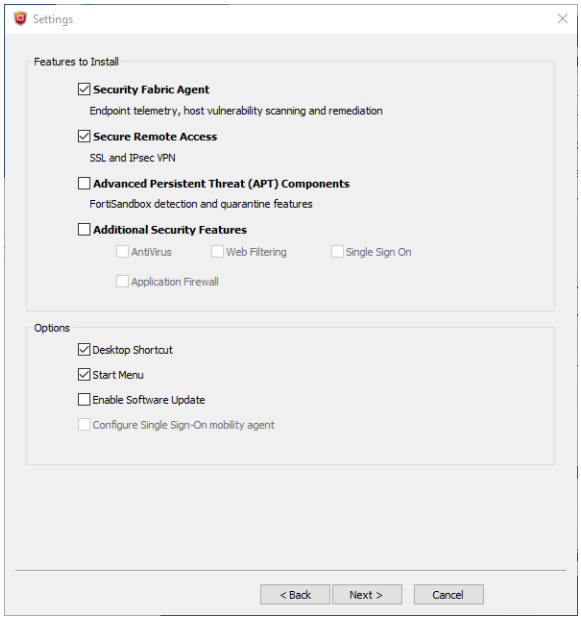
Windows has a hard limit of 260 characters on file path length. It is recommended to run the FortiClient Configurator Tool in a shallow directory structure, such as c:\temp\, to avoid hitting the hard limit.

To create a custom FortiClient installation file:

1. Double-click the *FortiClientConfigurator.exe* application file to launch the tool. The *Configuration File* page displays with the following options.

Select Config File (optional)	Select a FortiClient configuration file (`.conf`, `.sconf`) to include in the installer file.
Password	If the FortiClient configuration file is encrypted (`.sconf`), enter the password used to encrypt the file.
FortiClient Telemetry Gateway IP List (optional)	Select a FortiClient Telemetry gateway IP list to include in the installer file.

Locate and select the FortiClient configuration file on your management computer, and click *Next*. If you do not want to include settings from a configuration file, click *Skip* to continue. The *Settings* page displays.

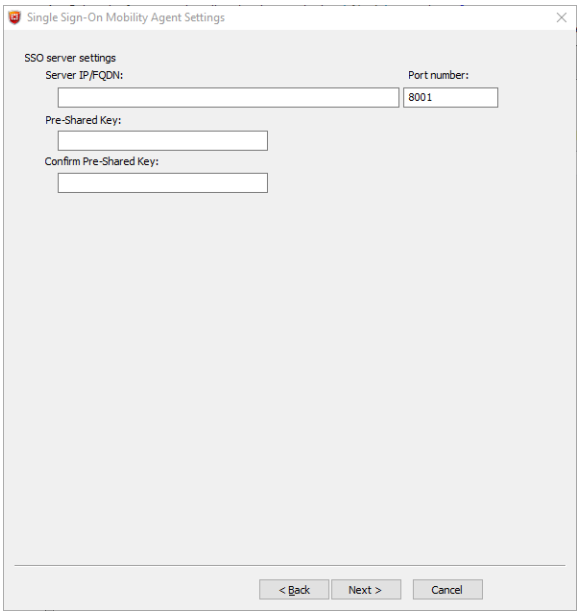


The following options are available for custom installations:

Features to Install

	Security Fabric Agent	Selected by default to support Fortinet Security Fabric. FortiClient Telemetry is always installed to support integration of FortiClient into the Security Fabric as follows: • Participate in compliance • Send user ID, avatar, and email address to FortiGate • Be managed by EMS Along with the Vulnerability Scan component (also included in this agent), this provides the Security Fabric administrators an overview of the endpoint state. Clear the checkbox to exclude the *Compliance* and *Vulnerability Scan* tabs from the FortiClient installation file.
	Secure Remote Access	Select to include SSL and IPsec VPN modules in the FortiClient installation file.
	Advanced Persistent Threat (APT) Components	Select to include FortiSandbox detection and quarantine modules in the FortiClient installation file.
	Additional Security Features	Select to include one or more of the following modules in the FortiClient installation file: • AntiVirus • Web Filtering • Single Sign On • Application Firewall
Options		
	Desktop Shortcut	Select to create a FortiClient desktop icon on the endpoint.
	Start Menu	Select to add FortiClient to the start menu on the endpoint.
	Enable Software Update	Select to enable FortiClient software updates via FortiGuard Distribution Network on endpoints.
	Configure Single Sign-On mobility agent	Select to configure Singe Sign-On mobility agent for use with FortiAuthenticator. You must select the *Single Sign On* checkbox in the *Features to Install* area first.

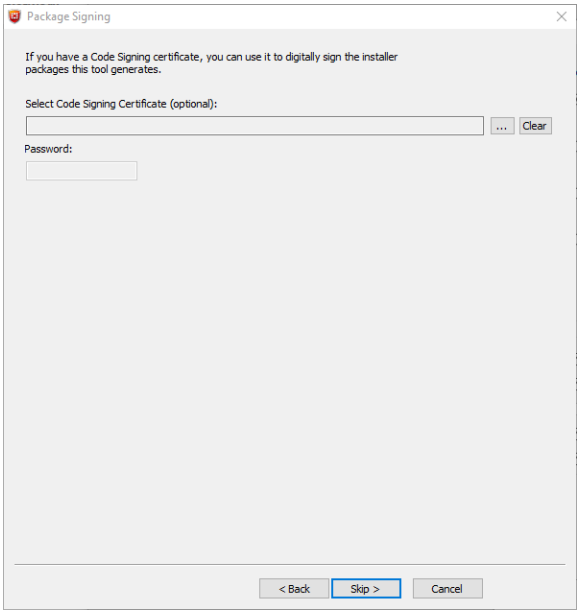
2. Select the features to install and options, and click *Next* to continue.
   If you selected the *Configure Single Sign-On mobility agent* checkbox, the *Single Sign-On Mobility Agent Settings* page displays.



3. Configure the following settings:

Server IP/FQDN	Enter the FortiAuthenticator server's IP address or FQDN.
Port number	Enter the port number. The default port is 8001.
Pre-Shared Key	Enter the FortiAuthenticator pre-shared key.
Confirm Pre-Shared Key	Enter the FortiAuthenticator pre-shared key confirmation.

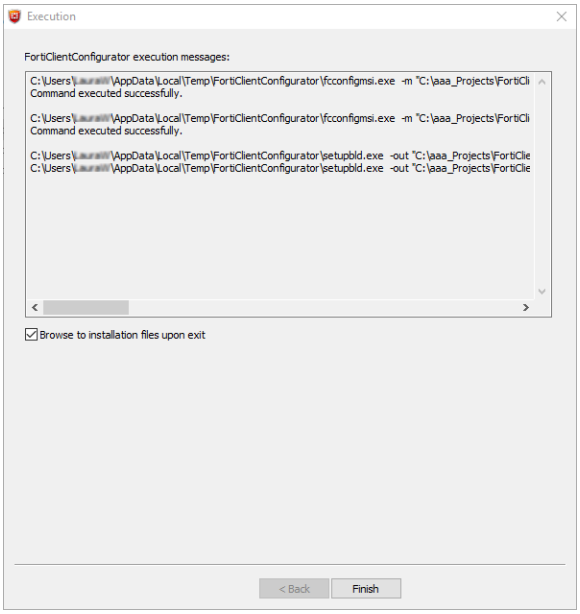
4. Click *Next* to continue. The *Package Signing* page displays.



5. Configure the following settings:

Select Code Signing Certificate (optional)	If you have a code signing certificate, you can use it to digitally sign the installer package this tool generates.
Password	If the certificate file is password protected, enter the password.

6. (Optional) Browse and select the code signing certificate on your management computer. If you do not want to digitally sign the installer package, select *Skip* to continue. The *Execution* page displays.



This page provides details of the installer file creation and the location of files for Active Directory deployment and manual distribution. The tool creates files for both 32-bit (x86) and 64-bit (x64) operating systems.

7. When you click *Finish*, the folder containing the newly created MSI file will open when the *Browse to installation files upon exit* checkbox is selected.

Before deploying the custom MSI files, it is recommended that you test the packages to confirm that they install correctly. An `.exe` installation file is created for manual distribution.

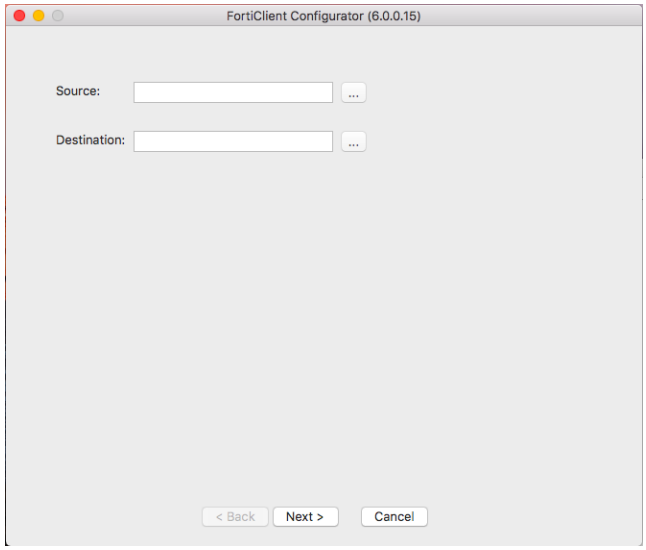
Installation files are organized in folders within the folder where you placed the *.exe* file for the FortiClient Configurator Tool. Folder names identify the type of installation files that were created and the creation date.

Using FortiClient Configurator Tool for macOS

To create a custom FortiClient installation file:

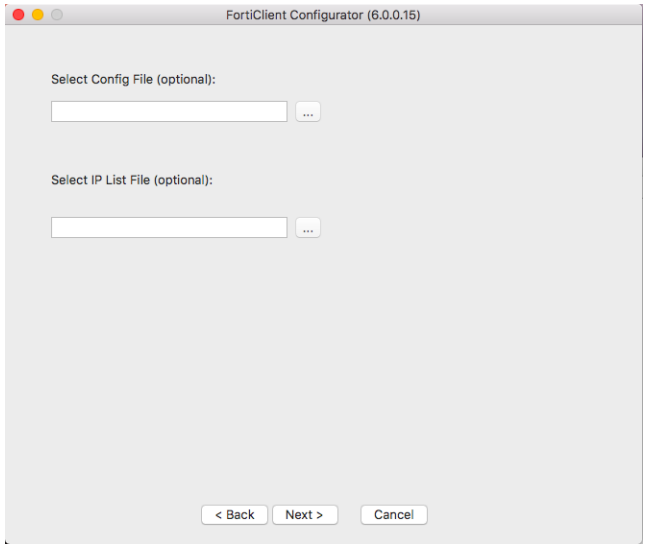
1. Double-click the *FortiClientConfigurator_6.0.2.xxxx.dmg* application file, and double-click the FortiClientConfigurator icon to launch the tool.

2. Configure the following settings, and click *Next*:



Source	Select the FortiClient Installer file on your management computer. You must use the full installer file, otherwise FortiClient Configurator Tool will fail to create a custom installation file. The FortiClient Installer version and FortiClient Configurator Tool version must match, otherwise the Configurator will fail to create a custom installation file.
Destination	Enter a name for the custom installation file and select a destination to save the file on your management computer.

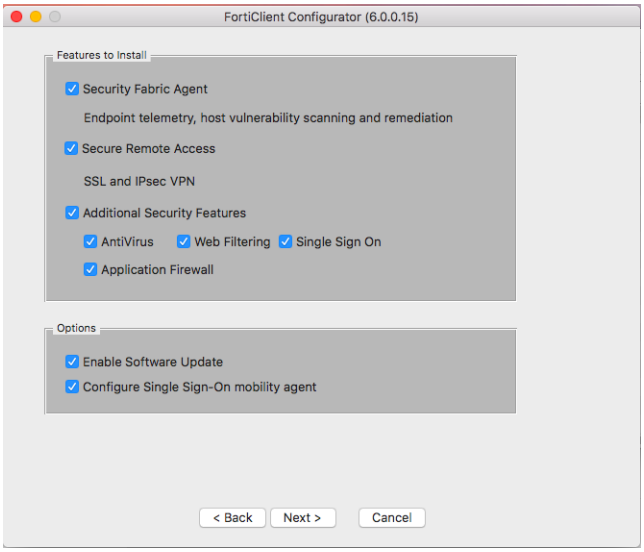
3. (Optional) Configure the following settings, and click *Next*:



Select Config File (optional)	Select a FortiClient configuration file (`.conf`, `.sconf`) to include in the installer file.

Password	If the FortiClient configuration file is encrypted (`.sconf`), enter the password used to encrypt the file.
Select IP List File (optional	Select a FortiClient Telemetry gateway IP list to include in the installer file.

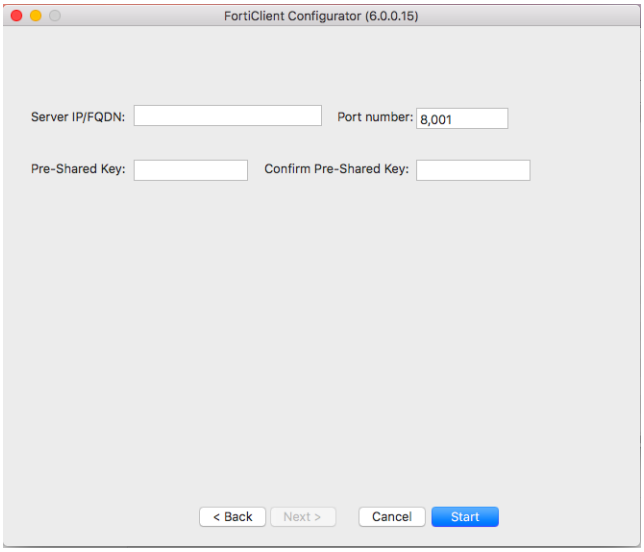
4. Configure the following settings, and click *Start*:



Features to Install		
	Security Fabric Agent	Selected by default to support Fortinet Security Fabric. FortiClient Telemetry is always installed to support integration of FortiClient into the Security Fabric as follows: • Participate in compliance • Send user ID, avatar and email address to FortiGate • Be managed by EMS Along with the Vulnerability Scan component (also included in this agent), this provides the Security Fabric administrators an overview of the state of the endpoint. Clear the checkbox to exclude the *Compliance* tab and *Vulnerability Scan* tab from the FortiClient installation file.
	Secure Remote Access	Select to include SSL and IPsec VPN modules in the FortiClient installation file.
	Additional Security Features	Select to include one or more of the following modules in the FortiClient installation file: • AntiVirus • Web Filtering • Single Sign On • Application Firewall
Options		

Enable Software Update	Select to enable FortiClient software updates via FortiGuard Distribution Network on endpoints.
Configure Single Sign-On mobility agent	Select to configure Singe Sign-On mobility agent for use with FortiAuthenticator.

5. If you selected the *Configure Single Sign-On mobility agent* checkbox, the *Single Sign-On Mobility Agent Settings* page displays. Configure the following settings:



Server IP/FQDN	Enter the FortiAuthenticator server's IP address or FQDN.
Port number	Enter the port number. The default port is 8001.
Pre-Shared Key	Enter the FortiAuthenticator pre-shared key.
Confirm Pre-Shared Key	Enter the FortiAuthenticator pre-shared key confirmation.

6. Click *Start*.
7. Click *Done*. You can now deploy the repackaged FortiClient `.dmg` file to your macOS systems.

Deploying custom FortiClient installation packages

This section includes information about deploying FortiClient (Windows) installation packages and FortiClient (macOS) installation files.

Deploying FortiClient (Windows) installation packages

After the FortiClient Configurator Tool generates the custom installation packages, you can use the custom installation packages to deploy FortiClient (Windows) software manually or using Active Directory. Both options can be found in the *.../FortiClient_packaged* directory. Files are created for both x86 (32-bit) and x64 (64-bit) operating systems.

If you are using Active Directory to deploy FortiClient (Windows), you can use the custom installer with the MST file found in the *.../ActiveDirectory* folder.

For manual distribution, use the `.exe` file in the *.../ManualDistribution* folder.

Deploying FortiClient (macOS) installation files

After the FortiClient Configurator Tool generates the custom installation file (`.dmg` file), you can use the custom installation file to deploy FortiClient (macOS) software.